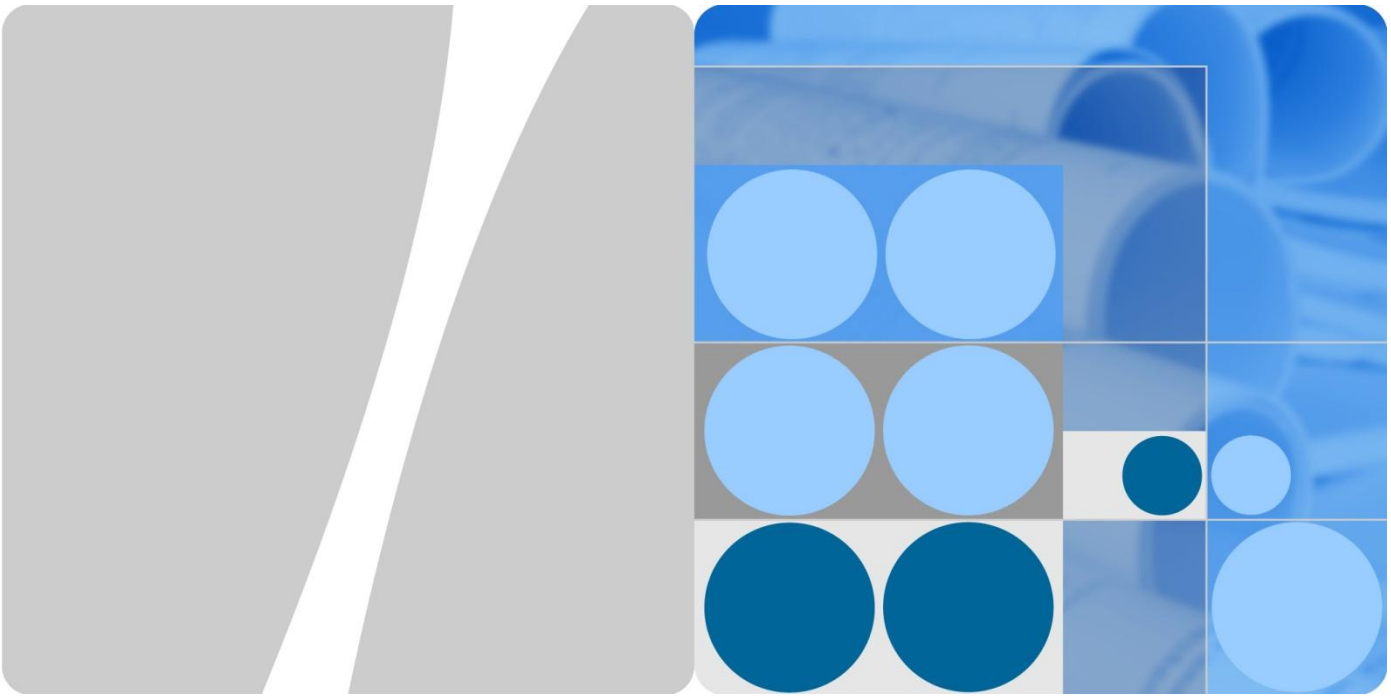


# IPSG Technology White Paper

**Issue** 01

**Date** 2012-09-10

**HUAWEI TECHNOLOGIES CO., LTD.**

### Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

## Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

# 1 IPSG

## About This Chapter

1.1 Introduction to IPSG

1.2 References

1.3 Principles

1.4 Applications

## 1.1 Introduction to IPSG

### Definition

IP Source Guard (IPSG) defends against source address spoofing attacks.

### Purpose

Some attacks on networks aim at source IP addresses by accessing and using network resources through spoofing IP addresses, stealing users' information or blocking authorized users from accessing networks. IPSG can prevent source address spoofing attacks.

### Benefits

- IP source guard prevents source IP address spoofing attacks and reduce maintenance costs.
- IP source guard improves network security and stability and defend against source IP address spoofing attacks.

## 1.2 References

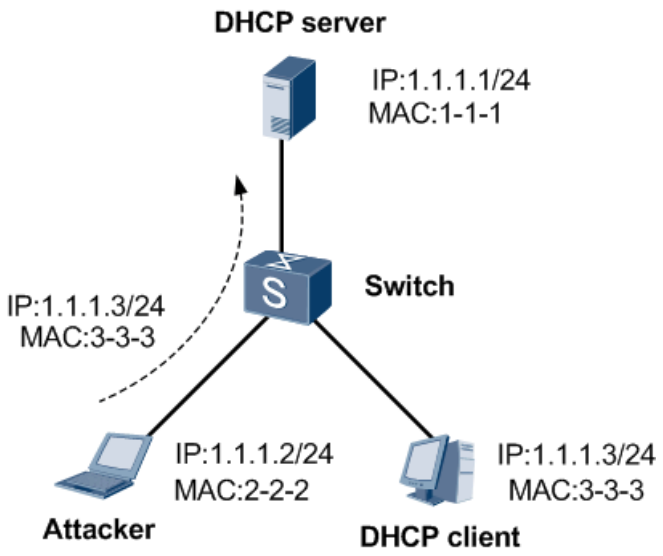
NONE

# 1.3 Principles

IPSG enables the device to check IP packets against dynamic and static DHCP snooping entries. Before the device forwards an IP packet, it compares the source IP address, source MAC address, interface, and VLAN information in the IP packet with entries in the binding table. If an entry is matched, the device takes the IP packet as a valid packet and forwards an IP packet. Otherwise, the device takes the IP packet as an attack packet and discards the packet.

As shown in Figure 1-1, an attacker sends bogus packets to modify the outbound interface in the MAC address table on the Switch. Then replies are sent from the server to the attacker.

**Figure 1-1** IP/MAC address spoofing attack




To prevent these attacks, you can configure IPSG on the Switch to check incoming IP packets against the binding entries. IP packets that match the binding entries are forwarded, and IP packets that do not match the binding entries are discarded.

## IPSG Check Items

IPSG enables the device to check IP packets against the binding entries. The check items contains the source IP address, source MAC address, VLAN ID, and interface number. The device supports IPSG to check the combination of the following items:

In the interface view:

- Interface and IP address
- Interface and MAC address
- Interface, IP address, and MAC address
- Interface, IP address, and VLAN ID
- Interface, MAC address, and VLAN ID
- Interface, IP address, MAC address, and VLAN ID

In the VLAN view:

- VLAN ID and IP address
- VLAN ID and MAC address
- VLAN ID, IP address, and MAC address
- VLAN ID, IP address, and interface
- VLAN ID, MAC address, and interface
- VLAN ID, IP address, MAC address, and interface

1. Configuring IP source guard in a VLAN

- Enable IP packet check.

```
[Switch] vlan 100
[Switch-vlan100] ip source check user-bind enable
```

- Configure IP packet check items.

# Check whether the source IP address of an IP packet matches a binding entry.

```
[Switch-vlan100] ip source check user-bind check-item ip-address mac-address
[Switch-vlan100] quit
```

- Run the display ip source check user-bind command to check the IP packet check configuration.

```
[Switch] display ip source check user-bind
  ------------------------------------------------------------

  IPSG VLAN ID       : 100

  IPSG check items    : IP | MAC
```

**IP | MAC** indicates that the source IP address and source MAC address are checked.

2. Configuring IP source guard on an interface

- Enable IP packet check.

```
[Switch] interface gigabitethernet 1/0/1
[Switch- GigabitEthernet1/0/1] ip source check user-bind enable
```

- Configure IP packet check items.

# Check whether the source IP address of an IP packet matches a binding entry.

```
[Switch- GigabitEthernet1/0/1] ip source check user-bind check-item ip-address mac-address
[Switch-vlan100] quit
```

- Run the **display ip source check user-bind** command to check the IP packet check configuration.

```
[Switch] display ip source check user-bind
  ------------------------------------------------------------

  IPSG interface      : GigabitEthernet1/0/2

  IPSG check items    : IP | MAC

  IPSG alarm         : Enable

  IPSG alarm threshold : 360
```

**IP | MAC** indicates that the source IP address and source MAC address are checked.

### IPSG Binding Table

IPSG supports the dynamic binding table and static binding table.

- After the DHCP snooping function is enabled for DHCP users, the binding table is dynamically generated for the DHCP users.
- If user IP addresses are configured statically, static binding entries are configured manually.

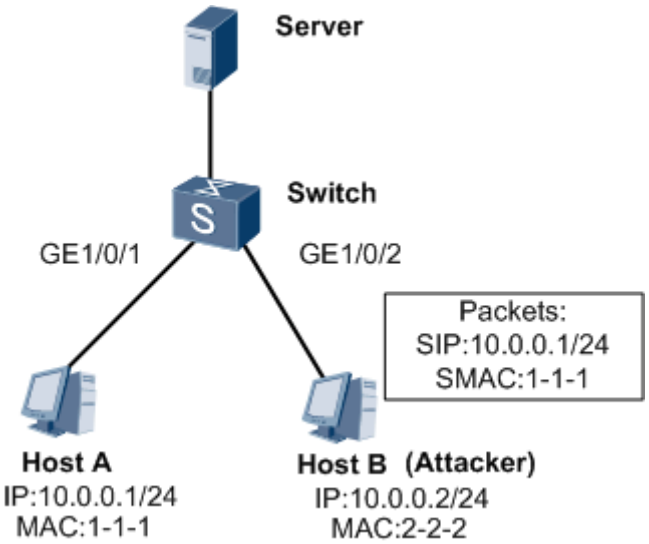
## 1.4 Applications

### 1.4.1 Typical Network of IPSG

As shown in Figure 1-2, HostA and HostB are connected to GE1/0/1 and GE1/0/2 on the Switch respectively. It is required that HostB not forge the IP address and MAC address of HostA and IP packets from HostA be sent to the server.

The enterprise is required to enable IP packet check on the two interfaces of Switch and configure static binding entries on HostA.

**Figure 1-2** Networking diagram for configuring IPSG




# Configuration file of Switch

```
#
  user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface
GigabitEthernet 1/0/1 vlan 10
#
interface GigabitEthernet 1/0/1
 ip source check user-bind enable
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
```

```
#
interface GigabitEthernet 1/0/2
 ip source check user-bind enable
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
#
return
```